



relation entre les ordinateurs et les mathématiciens. Ce n'est pas la première fois qu'un assistant de preuve est utilisé, mais c'est la première fois qu'une preuve mathématique (ou, tout au moins, une partie) n'a pas été vérifiée par des humains à l'exception de ses auteurs, mais uniquement par une machine. Cet événement est loin d'être anodin, et son impact a été amplifié par la réputation de Peter Scholze dont la qualité des travaux, à l'interface de l'arithmétique et de la géométrie, lui a valu de recevoir la médaille Fields en 2018, à seulement 30 ans.

UNE COMPÉTITION ?

Il est probable que l'influence de Peter Scholze, qui admet que la certification mécanique est un complément utile de son intuition, donnera un coup de pouce aux programmes de formalisation. Certains mathématiciens et de nombreux informaticiens se félicitent de cette évolution, qu'ils attendent depuis longtemps. Mais il existe aussi une vision selon laquelle la formalisation fondée sur l'informatique est un premier pas vers une version des mathématiques où les machines rejoignent les êtres humains, d'abord comme collègues, puis finissent par les dépasser. En 2020, lors d'une conférence, Christian Szegedy, chercheur chez Google, a évoqué des projets pour créer «une machine capable d'un raisonnement mathématique du niveau d'un humain d'ici à dix ans». Et les exemples du superordinateur Deep Blue, champion d'échecs, et plus récemment du programme AlphaGo, qui a atteint un niveau incomparable au jeu de go par autoapprentissage, sont cités comme la preuve que dans la compétition entre mathématiciens humains et mécaniques les premiers seront inévitablement perdants. Ces espoirs et craintes sont-ils réalistes ? Quelle sera alors la place des mathématiciens dans cette nouvelle distribution des rôles ?

Depuis longtemps, les machines ont une place importante en mathématiques. Le recours intensif aux systèmes mécaniques comme outil de calcul arithmétique et astronomique est bien documenté depuis l'Antiquité. Les premières machines à calculer modernes ont été inventées au ^{xvii}^e siècle sous l'impulsion de Pascal (avec la «Pascaline») et de Leibniz (avec sa «machine arithmétique», théorisée mais non fonctionnelle), considérés comme des pionniers à la fois du calcul mécanique et du développement des mathématiques modernes. Ces dispositifs ont facilité la résolution d'opérations complexes, libérant les chercheurs qui consacraient davantage de temps à leurs réflexions plutôt qu'aux fastidieuses lignes de calculs.

L'étape suivante a été le développement de la théorie du calcul par ordinateur. Celle-ci est née de façon surprenante durant une période de grande remise en question des fondements des mathématiques. Au début du ^{xx}^e siècle, David

Hilbert a été à l'initiative d'un programme nommé «le formalisme», dont le but était de rendre les mathématiques capables de vérifier l'exactitude de leur propre raisonnement. Hilbert avait observé qu'un énoncé mathématique pouvait être réécrit sous la forme d'une chaîne de symboles, et qu'une preuve était équivalente à une suite de transformations de ces chaînes selon les règles admises de la logique (comme dans le système de Bertrand Russell et Alfred Whitehead présenté dans leur livre *Principia Mathematica*). De la même manière qu'on peut calculer les solutions de certains types d'équations polynomiales, ou d'équations différentielles, à partir de la forme de l'équation en question, Hilbert a proposé que l'existence d'une preuve d'un théorème pouvait se déduire de la forme du théorème dans un langage symbolique adapté. De ce point de vue, le raisonnement mathématique était une sorte de calcul.

Cependant, en 1931, Kurt Gödel a semé le trouble et mis un point d'arrêt au programme de Hilbert en formulant ses deux célèbres théorèmes d'incomplétude. Il a montré que dans tout cadre axiomatique donné, certaines questions sont fondamentalement indécidables. Il n'est donc pas toujours possible de prouver qu'un énoncé est vrai ou faux. Les conséquences de ces théorèmes ont inspiré une décennie de réflexion intensive sur la nature du calcul et du raisonnement mathématique. Certains acteurs clés dans cette histoire, tels Alan Turing, Alonzo Church, et John von Neumann, ont alors jeté les bases de la théorie, et ensuite de la réalisation concrète des ordinateurs numériques.

Sans surprise, les mathématiciens ont très vite adopté les ordinateurs après leur mise au point. La capacité des premiers ordinateurs numériques à exécuter rapidement et avec précision des calculs a été exploitée dans de nombreux problèmes pratiques, dont le plus marquant, à cette époque, est la conception et le déploiement de la bombe à hydrogène.

Les performances du calcul numérique ont aussi été décisives pour la recherche théorique en mathématiques, en particulier dans le domaine de la théorie des nombres. Au milieu des années 1960, le mathématicien Peter Swinnerton-Dyer notait l'avantage que procuraient ces machines: «Avec l'invention des ordinateurs électroniques, les calculs qui auparavant auraient été hors de portée sont maintenant faisables aisément, à condition qu'ils soient assez répétitifs. Il doit y avoir beaucoup de branches de la théorie des nombres dans lesquelles le calcul intelligemment dirigé fournirait des résultats précieux.»

L'histoire des mathématiques est riche en exemples d'intuition forgée grâce à des calculs. Swinnerton-Dyer pensait à des résultats comme le théorème des nombres premiers, qui indique que la proportion de nombres premiers (des

nombres qui n'ont aucun diviseur en dehors de 1 et eux-mêmes) inférieurs à un entier donné n est environ $n/\ln(n)$, où $\ln$ est le logarithme naturel. Au XIX^e siècle, c'est en explorant à la main la répartition des nombres premiers que Adrien-Marie Legendre et surtout Carl Friedrich Gauss ont suggéré cette formule. Grâce à cette recherche empirique, et en s'appuyant sur des techniques d'analyse mathématique sur les séries infinies, Jacques Hadamard et Charles Jean de la Vallée-Poussin ont démontré le théorème des nombres premiers de façon indépendante la même année, en 1896.

Gauss, le fondateur d'une grande partie des mathématiques théoriques modernes, était fier de sa capacité exceptionnelle de calcul. Mais il n'aurait pas fait le poids face aux ordinateurs (même ceux relativement primitifs évoqués par Swinnerton-Dyer). Ces nouvelles machines produisent rapidement de vastes collections de données que les mathématiciens analysent pour y déceler des tendances et formuler des conjectures.

UNE CONJECTURE ASSISTÉE PAR ORDINATEUR

C'est de cette façon qu'au début des années 1960 Swinnerton-Dyer et son collègue Bryan Birch ont énoncé une conjecture qui porte leur nom (conjecture de Birch et Swinnerton-Dyer, BSD) et qui est encore aujourd'hui une des plus importantes en théorie des nombres. Pour arriver à cette proposition, les deux chercheurs ont mené un grand nombre de calculs sur l'ordinateur EDSAC de l'université de Cambridge. La conjecture concerne l'existence de solutions rationnelles pour les courbes elliptiques, des équations cubiques à deux variables, comme $y^2 = x^3 - Dx$, où D est un nombre rationnel (voir l'encadré page 30). De façon générale, ces équations sont les plus simples pour lesquelles les méthodes élémentaires sont incapables de déterminer *a priori* si le nombre de solutions rationnelles est fini (comme pour $D = 1$) ou infini (comme pour $D = 25$). La question est de nature algébrique; la conjecture BSD donne une réponse conjecturale et caractérise les solutions.

L'article de Swinnerton-Dyer fournit d'excellents arguments théoriques pour croire la conjecture BSD, qui depuis l'an 2000 est un des problèmes du millénaire de l'institut Clay (avec à la clé un prix de 1 million de dollars pour celui qui fournira une preuve). Le texte explique également comment des arguments heuristiques ont guidé la formulation de la conjecture et ses raffinements ultérieurs. Cette conjecture n'aurait probablement pas été acceptée aussi vite sans la présence des données numériques que seuls les ordinateurs pouvaient produire.

Ces machines ont largement contribué au dynamisme et à la fertilité de la recherche en théorie des nombres. Ainsi, si BSD résiste encore,